FEDERAL TRADE COMMISSION

SPAM SUMMIT

THE NEXT GENERATION OF THREATS AND SOLUTIONS

# SPAM SUMMIT:
## THE NEXT GENERATION OF THREATS AND SOLUTIONS

A Staff Report by the Federal Trade Commission's
Division of Marketing Practices
November 2007

## TABLE OF CONTENTS

## EXECUTIVE SUMMARY

Spam is one of the most intractable consumer protection problems faced by computer users. For the past decade, the Federal Trade Commission has been steadfast in the fight against fraudulent and deceptive spam. The nature of spam, however, has shifted, and a new generation of malicious spam is on the rise. This shift is marked by a change in both spammers' methods and motives for sending spam.

In the early years, spammers used basic traceable computer scripts to mass market products via email. In tracking the communications path, law enforcement often could find and shut down illegal spamming operations. Spammers soon adopted various methods to conceal their identities, including, for example, "spoofing," which is the use of falsified email headers to disguise the origin of their email messages. Spammers also used creative strategies for obtaining email addresses, including "harvesting" – the automated collection of email addresses from public areas of the Internet. A recent FTC staff study finds that despite spammers' ongoing use of spoofing and harvesting techniques, ISPs' spam filters continue to serve a key role in reducing the amount of spam delivered to consumers' inboxes.[1]

In recent years, however, FTC staff has seen an explosion in another, more insidious technique for sending spam – the use of malicious bots. A malicious bot is a type of malware designed to infect a host computer and connect back to a central server or servers that act as a command and control ("C&C") center. In most instances, victims are unaware that their computers have been hijacked and turned into a bot or become part of a "botnet" – a network of

[1] *See* Appendix A. Email Address Harvesting and the Effectiveness of Anti-Spam Filters: A Report by the Federal Trade Commission's Division of Marketing Practices (Fall 2007) (illustrating that one ISP blocked 93% of spam, while another ISP blocked 78% of spam).

hijacked computers that enables spammers to send large volumes of spam anonymously and remotely. Botnets often are credited with increasing the volume of spam hitting the filters of email and Internet service providers ("ISPs").

FTC staff also has seen a change in the underlying motives for sending spam. This new generation of spam is no longer a mere annoyance to email recipients and a burden to ISPs; often it is a vector for criminal activity.[2] Clicking on a link in a malicious spam message may direct a consumer to a website that could dupe the consumer into divulging personally identifying information, including passwords and financial data. Malicious spam also can infect a consumer's computer with spyware or other types of malware, which can result in slowed computer performance; installation of key-logger software that can record and report a consumer's every keystroke; the spread of computer viruses; and the hijacking of a consumer's computer for use in a botnet.

It is difficult to quantify malicious spam and its effects, and the landscape is constantly changing; however, some sobering statistics about the criminal nature of malicious spam include:

- According to Postini, "more than one million internet protocol (IP) addresses are

[2] *See e.g.,* Hughes, Day 1 at 29 (stating that spam has become more insidious today with phishing and other attacks); Grasso, Day 1 at 36 (stating that, in his law enforcement experience, he is seeing less spam that is used for advertising purposes, and more spam that is used for phishing or some type of malicious activity); and Stiles, Day 1 at 38 (stating that the nature of email has become more criminal).

The Spam Summit transcripts are available at http://www.ftc.gov/bcp/workshops/spamsummit/index.shtml. References to the transcript are identified by the name of the panelist, followed by the day on which the transcript testimony was provided (i.e., either Day 1 or Day 2 of the Summit), followed by the page number.

coordinating spam and virus attacks each day;"[3] and "more than 50,000 infected computers are attacking at any particular point in time."[4]

- According to MessageLabs, phishing emails intercepted in May 2007 accounted for 78.9 percent of malicious email traffic.[5]

On July 11 and 12, 2007, FTC staff convened a two-day workshop, "Spam Summit: The Next Generation of Threats and Solutions," to assess the impact of malicious spam on consumers, and to explore steps that stakeholders should take to mitigate the harmful effects of malicious spam.[6] Summit panelists confirmed that the nature of spam has changed, as it has become a significant, global vector for malware and financial crime. The nearly 50 panelists worked through a comprehensive nine-panel agenda that: defined the malicious spam problem; identified methods used for sending malicious spam; explored the malware economy; identified threats that malicious spam poses to emerging platforms such as mobile devices and social networking websites; examined countermeasures for law enforcement; developed educational tips for empowering consumers; identified best practices for legitimate email marketers; and explored strategies for reducing the impact of malicious spam.

To combat this new generation of spam, FTC staff will continue to bring civil law

[3] 2007 Postini Communications Intelligence Report, "The Communications Intelligence Gap: New Survey Uncovers Dramatic Gap Between Business Readiness and Increased Threats to Electronic Communications," available at http://www.postini.com/whitepapers/?WPID=43&src=GWT.

[4] *Id.*

[5] MessageLabs Intelligence Report: May 2007, "Spam Spikes – The Battering Ram of Spam", available at http://www.messagelabs.com/intelligence.aspx.

[6] *See* Agenda at Appendix B.

enforcement actions as appropriate and renew efforts to work with stakeholders in the anti-spam and anti-phishing communities. Specifically, FTC staff will work with stakeholders to:

- heighten collaboration among criminal law enforcement and industry;
- intensify efforts to deploy technological tools; and
- promote the continued development and dissemination of effective educational materials for consumers and businesses.

This report provides an overview of the FTC's role in the fight against fraudulent spam and phishing, explores key themes that emerged from the Summit, and identifies steps that stakeholders can take to mitigate the harms that result from malicious spam and phishing.

## I. The FTC's Role in the Fight Against Fraudulent Spam and Phishing

Beginning in 1997, the Commission has pursued an aggressive anti-spam program through law enforcement actions, consumer and business education efforts, research that has informed spam policy, public workshops and by spurring the development of industry-driven technology.

As of November 2007, the Commission has brought over 90 law enforcement actions, targeting a host of unfair and deceptive practices, relating to spam, including three cases that targeted phishing.[7] Phishing is a form of online identity theft that uses deceptive spam to trick consumers into divulging sensitive or personal information, including credit card numbers and

[7] *FTC v. Zachary Keith Hill*, Civ. Action No. H03-5537 (S.D.Tex. 2003), available at http://www.ftc.gov/opa/2004/03/phishinghilljoint.shtm; *FTC v. _______, an unnamed minor,* Civ. Action No. 03-5275 (C.D.Cal. 2003), available at http://www.ftc.gov/opa/2003/07/phishing.shtm; *FTC v.______, an unnamed minor,* Civil Action No. 04-2086 (E.D.N.Y. 2004), available at http://www.ftc.gov/os/2004/06/040518stipaminorbyhisparents.pdf.

other financial data. In these phishing cases, the FTC charged the defendants with violating the FTC Act, which prohibits unfair and deceptive practices, and the Gramm-Leach-Bliley Act, which protects the privacy of consumers' sensitive financial information.

Phishing is a criminal endeavor that is best suited for criminal law enforcement. Criminal enforcement agencies can obtain from ISPs crucial evidence that the Commission, as a civil agency, is prohibited from obtaining under the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. §§ 2510 et seq., 2701 et seq.). For example, in one phishing case, *FTC v. Zachary Hill*, the Department of Justice brought a parallel criminal case leading to a 46-month prison sentence for the defendant.[8]

Since the implementation of the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"),[9] the Commission has brought nearly 30 law enforcement actions focusing on the core protections that the CAN-SPAM Act provides to consumers: opt-out mechanisms that function; message headers that are non-deceptive; and protections against sexually-explicit spam. Eighty percent of the Commission's spam cases have alleged violations of the opt-out requirement, and more than 50 percent have alleged that email headers were deceptive. For example, in *Jumpstart Technologies*,[10] the Commission alleged that

[8] *U.S.A. v. Zachary Hill,* Plea Agreement (2004), available at http://www.ftc.gov/os/caselist/0323102/0323102zkhill.shtm. In other phishing cases, Commission staff worked closely with other criminal law enforcement agencies, including the Federal Bureau of Investigation, the United States Attorney for the Eastern District of Virginia's Computer Hacking and Intellectual Property Squad, the United States Postal Inspection Service and the Los Angeles District Attorney's High Technology Crimes Unit.

[9] 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037.

[10] *FTC v. Jumpstart Technologies*, Consent Decree and Order for Civil Penalties and Injunctive and Other Relief (2006), available at http://www.ftc.gov/os/caselist/0423176/0423176JumpstartTechnologiesConsentDecree.pdf.

the subject lines of the defendant's emails falsely indicated that a recipient's friend was sending free tickets, and many people who tried to opt out of the promotion continued to receive similar emails for weeks afterward. Under the settlement agreement, the defendant paid a $900,000 civil penalty for violating the CAN-SPAM Act, the largest penalty yet for illegal spam.

Similarly, in 2007, the Commission pursued another company, Adteractive, that used deceptive subject lines in spam to market purportedly "free" products to consumers.[11] In *Adteractive*, the Commission alleged that the companies violated the CAN-SPAM Act by using deceptive subject lines, and violated the FTC Act by failing to clearly and conspicuously disclose that, in many instances, consumers must spend money or incur other obligations to obtain "free" items.

In addition, some of the Commission's recent cases have highlighted various techniques used by spammers to mask their identities, including the use of botnets. For instance, in *FTC v. Dugger*,[12] the Commission alleged that the defendants relayed sexually-explicit commercial emails through other people's home computers without their knowledge or consent in violation of the CAN-SPAM Act. The settlement with the defendants required them to relinquish their ill-gotten gains and bars them from violating CAN-SPAM and the Adult Labeling Rule.[13] The settlement also requires that before the defendants use a third party's computer to send spam, they must obtain authorization from the computer's owner and inform the owner how the

[11] *FTC v. Adteractive,* Stipulated Final Judgment for Civil Penalties and Permanent Injunctive Relief (2007), available at http://www.ftc.gov/opa/2007/11/free.shtm.

[12] *FTC v. William Dugger et. al*, Final Judgment and Order for Permanent Injunction (2006), available at http://www.ftc.gov/os/caselist/0523161/060731duggerfinaljdgmnt.pdf.

[13] Adult Labeling Rule, 16 C.F.R. Part 316.4.

computer will be used.

The Commission's law enforcement cases also address the increasingly global nature of spam. In October 2007, the Commission brought *FTC v. Spear Systems, Inc.*,[14] its first case using tools under the U.S. Safe Web Act ("SAFE WEB"),[15] to stop spammers operating domestically and from Canada and Australia. The Commission alleged that the defendants violated the CAN-SPAM Act by initiating commercial emails that contained false "from" addresses and deceptive subject lines, and failed to provide an opt-out link or physical postal address. In *Spears Systems*, the Commission's authority under SAFE WEB enabled staff to advance the case by obtaining key information from Canadian and Australian authorities.

In addition to pursuing law enforcement actions, the Commission sponsors an innovative multimedia website, OnGuardOnline, designed to educate consumers about basic computer security.[16] The website provides information on several Internet-related topics, including phishing, spyware, and spam. For example, a recent addition to the website includes consumer tips on how to protect one's computer from becoming part of a botnet.[17]

The Commission also conducts research to explore how spam affects consumers and

[14] *FTC v. Spear Systems, Inc.*, Temporary Restraining Order (Oct. 2007), available at http://www.ftc.gov/os/caselist/0723050/index.shtm.

[15] U.S. SAFE WEB Act of 2006, Pub. L. No. 109-455, 120 Stat. 3372.

[16] The FTC developed OnGuardOnline in partnership with several other governmental agencies and many industry participants in the technology sector. The website is branded independently of the FTC so that other organizations may duplicate the information and disseminate it more widely to relevant audiences. Since its launch in 2005 through October 2007, OnGuardOnline has attracted more than 5 million visits.

[17] *See* www.onguardonline.gov and "*Botnets and Hackers and Spam (Oh, My!)*," available at http://onguardonline.gov/botnet.html.

online commerce. These research projects include staff-driven inquiries, such as the "False Claims in Spam Study,"[18] a study of the 100 top electronic retailers' compliance with the opt-out provisions of the CAN-SPAM Act,[19] and a study investigating the efficacy of filters employed by Internet and email service providers (the "Harvesting and Filtering Study").[20] Commission staff also has submitted four reports to Congress pursuant to the CAN-SPAM Act.[21]

In a study concluded in the fall of 2007, Commission staff replicated the work of the 2005 Harvesting and Filtering Study. The 2007 study found that one ISP effectively prevented the delivery of 93 percent of spam, while another ISP successfully blocked 78 percent of the spam.[22] These results suggest that spam-filtering technologies offered by Internet and email service providers continue to serve as integral tools in preventing spam from reaching consumers' inboxes.

The Commission also has played an active role in encouraging the development of

[18] False Claims in Spam: A Report by the Division of Marketing Practices (April 2003), available at http://www.ftc.gov/reports/spam/030429spamreport.pdf.

[19] Top Etailers' Compliance With CAN-SPAM's Opt-Out Provisions: A Report by the Federal Trade Commission's Division of Marketing Practices (July 2005), available at http://www.ftc.gov/reports/optout05/050801optoutetailersrpt.pdf.

[20] *See e.g.,* Email Address Harvesting and the Effectiveness of Anti-Spam Filters A Report by the Federal Trade Commission's Division of Marketing Practices (Dec. 2005), available at http://www.ftc.gov/opa/2005/11/spamharvest.pdf.

[21] National Do Not Email Registry Report to Congress (June 2004); A CAN-SPAM Informant Reward System: A Report to Congress (Sept. 2004); Subject Line Labeling As a Weapon Against Spam: A CAN-SPAM Act Report to Congress (June 2005); and Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress (Dec. 2005).

[22] *See* Email Address Harvesting and the Effectiveness of Anti-Spam Filters: A Report by the Federal Trade Commission's Division of Marketing Practices (Fall 2007) at Appendix A.

industry-driven technological tools to address the problem of spam. For example, in 2004, the Commission together with the Department of Commerce's National Institute of Standards and Technology ("NIST"), conducted a two-day Email Authentication Summit to spur the development of domain-level email authentication technologies. Over 300 people attended the Summit, including representatives from ISPs, small and large businesses, consumer groups, and technology firms.

Additionally, the Commission has hosted workshops to explore with stakeholders the most effective mechanisms for stopping spam. In 2003, the Commission hosted its Spam Forum workshop, which explored issues concerning unsolicited commercial electronic mail messages and various federal legislative proposals for addressing the spam problem.[23]

## II. Spam Summit Overview

In July 2007, FTC staff held its latest workshop, "Spam Summit: The Next Generation of Threats and Solutions," to examine the evolution of spam as a vehicle for malware and phishing, and to develop strategies for mitigating its effects.[24] The Summit convened experts from the business, government, and technology sectors, as well as consumer advocates and academics.

Generally, the data presented at the Summit suggest that while spam has had some ill-effects on consumer trust, consumers continue to use email on a wide scale and increasingly

[23] See Spam Forum 2003 website, available at http://www.ftc.gov/bcp/workshops/spam/index.shtml.

[24] The report is generally based on the record of the workshop, FTC studies, and published industry data. A copy of the agenda is attached as Appendix B. The Spam Summit transcripts are available at http://www.ftc.gov/bcp/workshops/spamsummit/index.shtml. References to the transcript are identified by the name of the panelist, followed by the day on which the transcript testimony was provided (i.e., either Day 1 or Day 2 of the Summit), followed by the page number.

exercise sophisticated management of their inboxes.[25] For example, one panelist opined that, in a decline from past years, only one in five consumers polled believes that spam is a problem for them.[26] Another panelist reported that two-thirds of computer users employ some type of spam-blocking software, and more computer users employ firewalls.[27] One panelist reported that 71 percent of email users utilize filters provided by their email service provider or employers, up from 65 percent two years ago.[28] Panelists further reported that industry is willing to take a proactive approach to combat spam and phishing on mobile devices and social networking websites.[29]

Despite these improvements, Summit panelists cautioned that other developments illustrate that malicious spam is a growing concern. For example, the majority of panelists observed that spam is increasingly used as a vehicle for committing financial crimes and that it causes significant harm to consumers and businesses. Panelists highlighted the critical roles of criminal law enforcement and public/private partnerships in increasing law enforcement's effectiveness, and the increasing use of domain-level email authentication as a foundation for more robust anti-spam technologies. The following sections of this report discuss key themes

[25] *See e.g.*, ESPC/ISPOS Email Survey Summary, available at http://www.ftc.gov/bcp/workshops/spamsummit/ESPC-and-Ipsos.pdf.

[26] S. Fox, Day 1 at 17 (stating that this drop could be due to a perceived decrease in the volume of the most offensive kind of spam containing explicit adult content). According to Fox, 52% of email users report having received a pornographic spam, which is down from 63% two years ago and 71% three years ago.

[27] J. Fox, Day 2 at 173.

[28] S. Fox, Day 1 at 17-18.

[29] *See* "Emerging Threats" panel, Day 1 at 211.

that emerged from the Summit, and identify the areas in which staff will work with stakeholders to help reduce the harmful effects of malicious spam and phishing.

## III. Spam Increasingly is a Vector for Criminal Activity

Panelists reached broad consensus on the underlying criminal nature of malicious spam and discussed strategies for combating malicious spammers.[30]

### A. The Majority of Malicious Spam is Sent Using Computers Infected with Malware

Panelists explored the underlying methods that cybercriminals use to distribute malicious spam. Panelists widely agreed that the use of bots is the key method for sending malicious spam,[31] and that bots are responsible for 95 percent of all spam.[32] A 2006 industry report indicates that nearly 12 million computers around the world are now compromised by bots.[33] Some panelists opined that the majority of bots today are located outside the U.S.[34] Panelists also described a growing phenomenon known as "fast flux." With fast flux, infected bot computers serve as proxies or hosts for malicious websites. The IP addresses for these sites are rotated regularly to evade discovery. For example, a phisher can deploy numerous and different

[30] Some panelists differentiated between commercial, legitimate email and malicious spam. Unlike senders of malicious spam, many senders of commercial, legitimate email seek to comply with CAN-SPAM and often adopt industry-set best practices. *See*, *e.g.,* Hughes, Day 1 at 75-76.

[31] Among applicable statutes, the use of bots can violate federal criminal provisions under the Computer Fraud and Abuse Act (18 U.S.C. §1030).

[32] *See* presentation of "Evolving Methods for Sending Spam and Malware" panel, Day 1, available at http://www.ftc.gov/bcp/workshops/spamsummit/presentations/Evolving-Methods.pdf.

[33] McAfee Virtual Criminology Report: Organised Crime and the Internet (Dec. 2006).

[34] St Sauver, Day 1 at 110; Peterson, Day 1 at 148; Ramasubramanian, Day 1 at 149.

IP addresses for a single phishing campaign, foiling the efforts of ISPs and law enforcement seeking to stop these campaigns by dismantling a single web site. Despite these challenges, the record reflects that at least one ISP does take proactive measures to detect and disconnect "fast flux" web sites from a portion of its network.[35]

### B. Spam Often is Used to Propagate Financial Cybercrime

Summit panelists identified spam as the primary gateway for cybercriminals to execute phishing attempts and other financial crimes. Further, a recent report from the Anti-Phishing Working Group ("APWG") reveals a dramatic increase in the number of websites either knowingly or unwittingly hosting "crimeware code," which is code designed to collect information about end-users for the purpose of stealing the users' personal information, including their financial data.[36]

Panelists opined that the availability of phishing software and crimeware code has made it easier for less sophisticated criminals to launch malicious spam and phishing campaigns. For example, one panelist stated that a community of malware providers offers a $17 spam-bundled spyware kit that enables attackers to disseminate spyware via spam.[37] Reportedly, the spyware kit even includes technical support.[38] According to a recent industry report, phishing toolkits,

[35] Romary, Day 2 at 143-144 (stating that AOL's ATDN customers were not participating in fast flux proxy networks because AOL used its ability to disconnect these customers from fast flux proxy networks). ATDN is a global Tier-1 IP backbone network used by AOL customers to transmit electronic mail and data. *See* http://www.atdn.net.

[36] APWG's Phishing Activity Trends Report for the Month of June 2007, available at http://www.antiphishing.org/reports/apwg_report_may_2007.pdf.

[37] Klein, Day 1 at 160.

[38] *Id.*

which are computer scripts that enable an attacker to automatically set up phishing web sites that spoof legitimate sites, also are available for purchase on the Internet.[39] One panelist noted that with a phishing toolkit, a phisher can create a phishing scheme within seconds that is ready to be launched.[40] This panelist noted that the price of such phishing toolkits has plunged significantly.[41] Bot rentals also are easy to obtain. One panelist stated that two jailed spammers — Jeanson James Ancheta and Christopher Maxwell — rented bots for $300 to $700 per hour.[42]

### C. Cybercrime Causes Significant Harm

A survey by *Consumer Reports* reveals that viruses, phishing, and spyware resulted in over $7 billion in costs to U.S. consumers in 2007.[43] The survey revealed further that computer infections prompted 850,000 U.S. households to replace their computers.[44] The costs to businesses also are high. One panelist reported that 80 percent of 639 businesses it studied experienced cybercrime-related losses, totaling $130 million.[45] In addition, the Federal Bureau

[39] "Symantec Internet Security Threat Report Trends for January–June 2007" available at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf. According to the report, the top three most widely used phishing toolkits were responsible for 42% of all phishing attacks detected during the reporting period.

[40] Hinrichsen, Day 1 at 167.

[41] *Id.* at 169.

[42] Klein, Day 1 at 156; *See also* Presentation of Andrew Klein, available at http://www.ftc.gov/bcp/workshops/spamsummit/presentations/Malware-Economy.pdf.

[43] Consumer Reports, "2007 State of the Net Survey" available at http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/state-of-the-net/0709_state_net.htm.

[44] *Id.*

[45] Mularski, Day 2 at 39.

of Investigation ("FBI") has identified over 200 government sites that are compromised and being used to send spam.[46] One panelist noted that these compromised government sites are a concern from a national security perspective.[47]

### D. Criminal Law Enforcement Can Play a Major Role

Panelists agreed that criminal law enforcement can and should play a significant role in the fight against malicious spam. One panelist advised that cybercrime is the third investigative priority of the FBI, behind only counter-terrorism and counter intelligence.[48] Currently, the FBI has a combination of 70 significant ongoing investigations that pertain to spam and phishing.[49] The FBI also has a "Slam-Spam Initiative," which brings together over 100 subject matter experts to work with the FBI. This initiative has identified 100 significant spamming operations.[50] Five of these spamming operations have been tied to organized crime.[51]

The FBI also works closely with the Department of Justice ("DOJ"). For example, one panelist described "Operation Botroast," a new FBI and DOJ joint initiative.[52] To date, "Operation Botroast" has resulted in charges against three spam schemes. In the first of these cases, the *Soloway* case, the defendant was indicted and charged with criminal CAN-SPAM

[46] *Id.* at 42.

[47] *Id.*

[48] Mularksi, Day 2 at 38.

[49] *Id.* at 42.

[50] *Id.*

[51] *Id.*

[52] Spivack, Day 2 at 25.

violations, wire fraud, mail fraud, and money laundering.[53] The defendant is alleged to have used botnets and other exploits to ricochet tens of millions of spam messages from the computers of unknowing computer users.[54] In the second case, the *Downey* case, the indictment charged that the defendant was hired by others to commit distributed denial of service ("DDoS") attacks on various competitors of the payor. The defendant is believed to have created the code and herded thousands of bot machines that on a regular basis committed DDoS attacks. The defendant entered a guilty plea in mid-June 2007. In the third case, the *Brewer* case, the defendant is alleged to have used a botnet to infiltrate hospital computers in the Chicago area. The defendant was indicted under 18 USC § 1030 for gaining access to medical information using bots.[55]

On November 29, 2007, the FBI and DOJ announced "Botroast II," which has led to three new indictments, guilty pleas from two previously charged bot operators, and the sentencing of three other cybercriminals, including a pair of men who launched a major phishing scheme targeting a Midwest bank that led to millions of dollars in losses.[56]

Another panelist from the U.S. Postal Inspection Service ("USPIS") identified "Operation Gold Phish" as another example of criminal law enforcement efforts.[57] Under this initiative, USPIS, the International Criminal Police Organization ("Interpol"), and international

[53] *Id.*

[54] *Id.*

[55] Spivack, Day 2 at 26.

[56] The FBI's press release is available at http://www.fbi.gov/page2/nov07/botnet112907.html.

[57] Crabb, Day 1 at 180.

law enforcement officers from more than a dozen different countries work together to uncover cybercriminals. In one instance, this initiative uncovered "Barracuda," an individual believed to be located outside the U.S., who is alleged to have hawked $300 malware kits that could be bundled with spam to disseminate computer viruses.[58]

Criminal law enforcers on the state level also are playing an active role in the fight against spam. One panelist from the Computer Crimes Unit of the Virginia Attorney General's office described a case against Jeremy Jaynes*,* who, at the time, was believed to be the eighth most prolific spammer in the world.[59] In the *Jaynes* case, prosecutors argued that the defendant sent fraudulent email messages to victims from all around the world, amassing a net worth of $22 million. Jaynes was convicted under Virginia's Anti Spam Act, which criminalizes the sending of unsolicited bulk email by fraudulent means, such as changing the header or routing information of an email to prevent recipients from contacting or knowing the identity of the sender.[60]

### E. Partnerships Between the Public and Private Sectors Can Make Criminal Law Enforcement More Effective

Of course, law enforcement cannot tackle the problem of malicious spam alone. Panelists provided numerous examples of the importance of partnerships between public and private sector entities in the fight against spam. One successful model featured at the Summit is the National Cyber-Forensics and Training Alliance, in which criminal investigators and industry analysts work together in the same physical location in Pittsburgh, Pennsylvania to

[58] Crabb, Day 1 at 181.

[59] Fishel, Day 2 at 11.

[60] Virginia Code § 18.2-152.3:1 (2003).

facilitate the exchange of critical information in real time.[61] Through this alliance, the FBI has been able to identify and prosecute some of the most serious cyber criminals, including those who distribute computer viruses, operate large botnets, and perpetrate phishing crimes. Other examples of partnerships between law enforcement and the private sector include Digital Phishnet and InfraGard. Digital Phishnet is a collaborative enforcement operation that unites industry leaders in technology, banking, financial services, and online retail services with law enforcement to combat phishing.[62] InfraGard is an alliance among the FBI, the information technology industry, and academia that has the goal of promoting the FBI's investigative efforts in the cyber arena.[63]

Due to the international nature of many of these threats, collaborative law enforcement efforts on a global scale also are critical. One panelist identified the Council of Europe Convention on Cybercrime as an international convention that aims to provide more tools for cooperation against threats posed by hacking and other computer-related crimes.[64] This panelist also mentioned the London Action Plan,[65] which is a network of the FTC, international law enforcement from more than 20 countries, and private sector participants, all working together to combat spam.[66]

[61] Grasso, Day 1 at 19.

[62] Mularski, Day 2 at 43.

[63] *See* http://www.infragard.net. *See also* Schneck, Day 2 at 278-279.

[64] Stevenson, Day 2 at 55;

[65] *Id.* at 56.

[66] One of the successes of the London Action Plan includes, for example, an initiative in 2005 to educate ISPs about bots.

## IV. Authentication and Other Technologies Can Help Counter Phishing and Other Forms of Malicious Spam

One of the most encouraging marketplace developments regarding email involves the creation of domain-level email authentication systems that are designed to combat the fundamental problem facing the email system today – the technological ability of spammers to send email anonymously. Summit participants uniformly agreed that email authentication is integral to the development of other technologies that can help counter phishing and other forms of malicious spam.

### A. Authentication Addresses a Key Flaw in Email's Protocol

Spam is made possible because the simple mail transfer protocol ("SMTP") used for email does not require an email message to contain accurate routing information, except for the intended recipient of the email. Therefore, a spammer may "spoof" or falsify some portions or all of the header of an email message, making it virtually impossible for ISPs and law enforcement to identify the true source of an illegal email message. Domain-level authentication technology addresses this problem by enabling a receiving mail server to know if an email was sent from an IP address that is registered to the purported sender. For example, if an email message purported to come from *abc@ftc.gov*, domain-level authentication would make it possible for a recipient to know if, in fact, the email came from the "ftc.gov" domain.

One of the current proposals in the marketplace, Sender ID, would require all email senders to publish in the domain name system ("DNS") the IP addresses from which they send email.[67] Receiving mail servers could then compare the IP addresses listed in the header of an

[67] Information about Sender ID is available online at http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx.

email message with the IP addresses in the DNS to "authenticate" the domain from which the message was sent.

Domain Keys Identified Mail ("DKIM"), the other authentication technology that is being widely deployed, is a signature-based mechanism for authenticating an email message.[68] One panelist highlighted advancements with DKIM, which include approval by the Internet Engineering Task Force ("IETF") as a standards-tracked protocol.[69] The panelist advised that this means that DKIM has been fully vetted by the IETF.

As authentication technologies continue to be adopted and implemented, ISPs, as part of their filtering and scoring systems, will give authenticated email a positive score and non-authenticated email a negative score. While lack of authentication alone may not prevent delivery of an email message, it will be an additional criterion applied by existing anti-spam filtering policies, making it more likely that non-authenticated messages will be blocked. Following the Summit, FTC staff learned that some ISPs have begun to apply negative scoring to unauthenticated email.[70]

Several trade associations, including the Email Service Provider Coalition ("ESPC"), the Direct Marketing Association ("DMA"), and the Interactive Advertising Bureau ("IAB"), require their members to authenticate their outgoing email. BITS, the technology policy division of the Financial Services Roundtable, has strongly recommended that its members adopt authentication

[68] Fenton, Day 2 at 89.

[69] *Id.*

[70] Lyris ISP Deliverability Report Card Q2 2007, available at http://www.lyris.com/resources/reports/deliverability_report_Q22007.pdf.

by the end of 2008.[71] Other entities such as the U.S. Chamber of Commerce and the Better Business Bureau also are beginning to encourage authentication.[72] Moreover, during the closing panel of the Summit, the FBI and InfraGard agreed to use InfraGard's membership to help small businesses authenticate their email messages.[73]

### B. Industry Data Demonstrate the Promise of Domain-level Authentication

Panelists agreed that email authentication is a critical building block for detecting spoofed email.[74] A panelist from Microsoft spoke of his company's experience with the use of its own SenderID technology in managing over 300 million consumer mailboxes. According to Microsoft, Sender ID authentication is helping to improve filtering, and is reducing the occurrence of false-positives, which is the inadvertent rejection of a legitimate email message.[75] The panelist reported that Hotmail is seeing an 85 percent reduction in false positives using SenderID authentication and reputation data.[76] The data from Hotmail, according to the panelist, also indicate that SenderID and reputation data have assisted in detecting 95 percent of phishing exploits.[77] This panelist reported that the use of SenderID is not limited to Hotmail; 45 percent

[71] Ingold, Day 2 at 232.

[72] Spiezle, Day 2 at 134.

[73] Grasso and Schneck, Day 2 at 278-280.

[74] Spiezle, Day 2 at 84; Fenton, Day 2 at 91; Cahill, Day 2 at 100.

[75] *Id.* Reputation data and reputation-based scoring are discussed infra on p. 23.

[76] *Id.*

[77] *Id.* at 85.

of legitimate email is authenticated using the SenderID protocol, and nearly 12 million domains worldwide are SenderID compliant.[78]

The utility of SenderID appears to be diminished, however, because some senders reportedly misconfigure their SPF records — the lists of authorized email-sending domains published in the DNS. For example, the SenderID specification allows an entity to publish its IP address records with a syntax declaring that anyone can send email from its domains. Records that are misconfigured in this manner offer no protection from spoofing because receiving ISPs have no way of determining whether a sender is actually authorized to send email on behalf of the domain holder.[79] One panelist reported that in a group of 1.5 million non-spamming senders, 27 percent were using SenderID, but 13 percent had misconfigured records.[80] For the SenderID authentication protocol to reach its full potential, the problem of misconfigured SPF records must be addressed by industry.

Like SenderID, DKIM is now being widely deployed. One panelist reported further that there are a variety of vendor email products available that support DKIM, and many more will

[78] *Id.* Moreover, panelists Spiezle and Fenton agreed that SenderID is compatible with the DKIM standard and that the two standards help to compensate for each other's strengths and weaknesses. Spiezle reported that 50% of all legitimate email worldwide is authenticated, using either SenderID, DKIM, or a combination of the two.

[79] Another concern is that, under the SenderID specification, some email senders fail to include all authorized domains that are used for sending email. An email sent from a server that is not published may be deleted, blocked or junked based on the receiving network or ISP's authentication policies. *See* http://download.microsoft.com/download/1/1/8/1184dafa-f1c6-4cd6-8fa1-0b06abbebd79/sdf_tips.pdf.

[80]Cahill, Day 2 at 106.

soon be available.[81] These products range from ones being intended for small and medium businesses to ones that can be used by large enterprises and service providers.[82] This panelist recognized Google Mail as currently signing its outbound email with DKIM, and mentioned that several financial institutions are leading the way in deploying DKIM because they see a real value in terms of protection of their brands and protection of their domain names.[83] The panelist stated that thus far, the proponents of DKIM - Cisco and Yahoo! - have valid DKIM signatures from over 20,000 domains.[84] Moreover, in October 2007, eBay and PayPal adopted DKIM technology that will enable Yahoo! Mail to block spam and phishing messages that purport to be from these companies.[85]

### C. Domain-level Authentication Improves the Effectiveness of Other Anti-spam Technologies

Much of the promise of domain-level email authentication technology lies in how it can vastly improve other anti-spam technologies. For instance, the utility of accreditation and reputation services will increase substantially when domain-level authentication systems are widely deployed. Accreditation services certify that a particular sender uses best practices. Reputation scoring looks at the practices of senders and assigns a reputation score depending on whether the messages sent appear to be spam or legitimate email.

[81] Fenton, Day 2 at 90.

[82] *Id.*

[83] *Id.*

[84] *Id.* at 91.

[85] Yahoo! Mail Press release (October 4, 2007), available at http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=267325.

ISPs' anti-spam filters can incorporate accreditation and reputation scores into their algorithms. Used in conjunction with domain-level authentication, a recipient's ISP could have a fair degree of certainty that an email that purports to be from an accredited sender or a sender with a positive reputation actually came from that sender.

Panelists agreed that reputation services are critical building blocks, and that reputation is an important component in minimizing the impact of spam in the inbox.[86] In one example, a panelist explained that in June 2007, his company analyzed 750 million distinct IP addresses sending email. The panelist stated that because 450 million of these IP addresses were "dynamic," they were probably bots.[87] The company conducted further tests and identified 99.8 percent of the senders as having a reputation of a spammer.[88] The panelist observed that reputation data are key for separating legitimate email from the majority of spam that is being received by ISPs.[89]

Another panelist described a reputation service that is a message tokenization system.[90] With this system, senders that are screened by the company purchase tokens that allow them to send a restricted number of email messages. Messages sent by these senders contain a digital

[86] Cahill, Day 2 at 99.

[87] Generally, a computer has a static IP address if it uses the same IP address each time that it connects to the Internet. Conversely, a computer has a dynamic IP address if the computer's IP address changes frequently. Panelist Cahill's comments suggest that one characteristic of a bot computer is its use of dynamic IP addresses.

[88] Cahill, Day 2 at 105-106.

[89] *Id.*

[90] Hirschman, Day 2 at 114.

signature.[91] Another panelist described a reputation system that focuses on an email privacy seal and a trusted download program.[92] The email privacy seal program certifies the email practices of websites that comply with standards of the program.[93]

Panelists agreed that email authentication and reputation services are useful tools for fighting bots because these tools limit the capabilities of the malefactors. One panelist stated that because spam is sent through bot networks comprised of thousands of computers, receiving networks need to pay attention to inbound email and investigate whether incoming email is authenticated or whether "throttling" would be appropriate.[94] The panelist described throttling as limiting the volume of email on a daily basis that can come into a network if it is not authenticated and has no reputation data.

Finally, one panelist stated that ISPs are in an advantageous position in terms of being able to detect and stop bots before they infect consumers' computers.[95] This panelist specifically stated that AOL, as an owner of an Internet access network that it leases to others, is able to observe a wide array of traffic patterns and to identify when bots attempt to connect from remote-controlled computers to the bots' master DNS servers. The panelist explained that, with this unique vantage point, AOL is able to disconnect bots by interrupting the attempted connections between the bot and the computers that remotely control the bots, thereby

[91] *Id*.

[92] Landesburg, Day 2 at 123-124.

[93] *Id.*

[94] Spiezle, Day 2 at 133.

[95] Romary, Day 2 at 144.

preempting many bot takeovers.[96]

## V. Next Steps

Based on the information provided by Spam Summit panelists, public comments submitted in response to the Spam Summit press release, and the Commission's own research and law enforcement experience, FTC staff proposes the following next steps to combat malicious spam and phishing.

### A. Stakeholders Should Heighten Collaboration Among Criminal Law Enforcement, Industry, and Other Stakeholders

The Summit record confirms that criminal authorities are best suited to tackle the problems of malicious spam and phishing. By collaborating with industry and working globally, the efforts of criminal law enforcement can only be heightened. Toward this end, stakeholders should maximize the effectiveness of partnerships among criminal law enforcement, industry, and other stakeholders in the fight against malicious spam, both domestically and abroad. In addition, the FTC will continue to bring civil law enforcement actions as appropriate.

### B. Stakeholders Should Intensify Efforts to Deploy Technological Tools

Authentication technologies are critical building blocks for other spam-fighting tools. Stakeholders have made significant strides in the deployment of these technologies. Staff will encourage continued industry-driven efforts to deploy authentication, and, in turn, work with stakeholders to: (1) encourage entities and associations to authenticate outbound email;[97] (2) educate senders about how to properly configure and authenticate their email; (3) urge ISPs to

[96] *Id.*

[97] For example, FTC staff is encouraged by InfraGard's pledge to help small businesses authenticate their email messages, and looks forward to seeing this program implemented.

further implement negative scoring for non-authenticated email; and (4) urge ISPs that have the ability to detect bot activity to stop bots immediately to prevent unauthorized access to consumers' computers by spammers and phishers.

### C. Stakeholders Should Continue to Develop and Disseminate Effective Educational Materials for Consumers and Businesses

Consumer and business education can have a significant impact in the fight against spam and phishing.[98] Because spam is an ever-evolving problem, stakeholders should revitalize efforts to educate consumers about how to protect their computers from online threats and improve methods for disseminating educational materials to consumers and businesses.[99] In addition, the Summit identified consumer-interfacing tools such as spam reporting buttons as valuable tools for ISPs and reputation service providers.[100] Accordingly, staff will encourage industry to continue to develop and fine-tune such tools.

[98] Recognizing the impact that consumer and business education can have in the fight against phishing, FTC staff intends to hold a half-day anti-phishing roundtable in the coming months.

[99] For example, following the Summit, staff worked with Citigroup, Inc. ("Citi"), a financial services company, to help Citi become an OnguardOnline partner. Citi now links to onguardonline.gov at http://financialeducation.citi.com/citigroup/financialeducation/resources.htm.

[100] *See e.g.,* Hughes, Day 1 at 27 (stating that, according to a recent ESPC survey, consumers want more buttons, not less, and stating that many of the major email clients, web mail providers, and ISPs offer a report-a-spam button); Libbey, Day 2 at 193 (stating that the spam button is an immensely valuable feedback tool for Yahoo! Mail and encouraging all consumers to use the spam buttons provided by their service provider); Romary, Day 2 at 128-129 (stating that AOL's "report spam button" led to consumer feedback that could be used to modify AOL's spam blocking mechanisms); Cahill, Day 2 at 97 (stating that spam button data are used to develop reputation data about a sender, which ultimately are used to determine whether or not a sender's email is delivered); Lane, Day 1 at 247 (stating that MySpace provides users of its social networking web site with a report spam button).

# Appendix A

## Email Address Harvesting and the Effectiveness of Anti-Spam Filters: A Report by the Federal Trade Commission's Division of Marketing Practices Fall 2007

## I. Overview

This report replicates a 2005 study conducted by staff of the Federal Trade Commission ("FTC") to evaluate two aspects of spam in the current Internet environment. First, the study explored the current state of email address harvesting - the automated collection of email addresses from public areas of the Internet. Similar to the 2005 study, the current study found that addresses posted on websites were at risk of being harvested by spammers, but that postings on other website locations, such as chatrooms, message boards, social network sites, and video posting sites were far less likely to be harvested.

Second, the study explored the effectiveness of spam filtering by Internet Service Providers ("ISPs"). As with the 2005 study, the current study showed that the anti-spam filters utilized by two free web-based ISPs effectively blocked the vast majority of spam sent to harvested addresses.[101] The implication of this finding is that ISP spam filtering technologies continue to play an integral role in reducing the amount of spam messages delivered to consumers' inboxes.

## II. Methodology

To measure the prevalence of harvesting and the effectiveness of two major ISPs' anti-spam filters, FTC staff created 150 new undercover email accounts. FTC staff established 50 of

[101] The difference in results at the two ISPs demonstrates that results at different ISPs may not be the same. Thus, results of this study cannot be generalized to other ISPs.

these email addresses at an ISP that employs no anti-spam filtering technologies (the "Unfiltered Addresses") and 50 addresses at each of the two free web-based ISPs that pass incoming email through anti-spam filters ("Filtered ISP 1" and "Filtered ISP 2").

FTC staff then posted sets of three of these newly-created email addresses - consisting of an Unfiltered Address, an address at Filtered ISP 1, and an address at Filtered ISP 2 - on 50 Internet locations. The 50 Internet locations included websites controlled by the FTC and several popular message boards, blogs, chat rooms, social networking sites, video posting sites, and sites with user-generated content that had high hit/visit rates.

**Locations on Which Email Addresses Were Posted**

Graphic 1

| Type | Number |
|---|---|
| FTC Website Pages | 10 |
| Message Boards | 14 |
| Blogs | 7 |
| Chat Rooms | 3 |
| User Generated Content (including video posting sites) | 6 |
| Social Networking Websites | 10 |

After a two week period, and again three weeks later (after a five-week period), FTC staff tallied the total number of spam messages in the inbox of each of the email accounts. The receipt of messages by Unfiltered Addresses indicated whether harvesting had occurred. It also indicated whether the posting of these email addresses on different types of Internet locations - such as websites, message boards, blogs, chatrooms, social networking sites, video posting sites, and sites with user-generated content - resulted in different levels of harvesting. In addition, because at each site the FTC staff had posted a triad of email addresses - one from each of the three groups we had created (Unfiltered ISP, Filtered ISP 1 and Filtered ISP 2) - FTC staff was able to calculate the percentage of spam messages blocked by the two ISPs' spam filters by comparing the number of messages received in each of the Unfiltered Addresses to the number of message received in Filtered ISP 1 and in Filtered ISP 2.

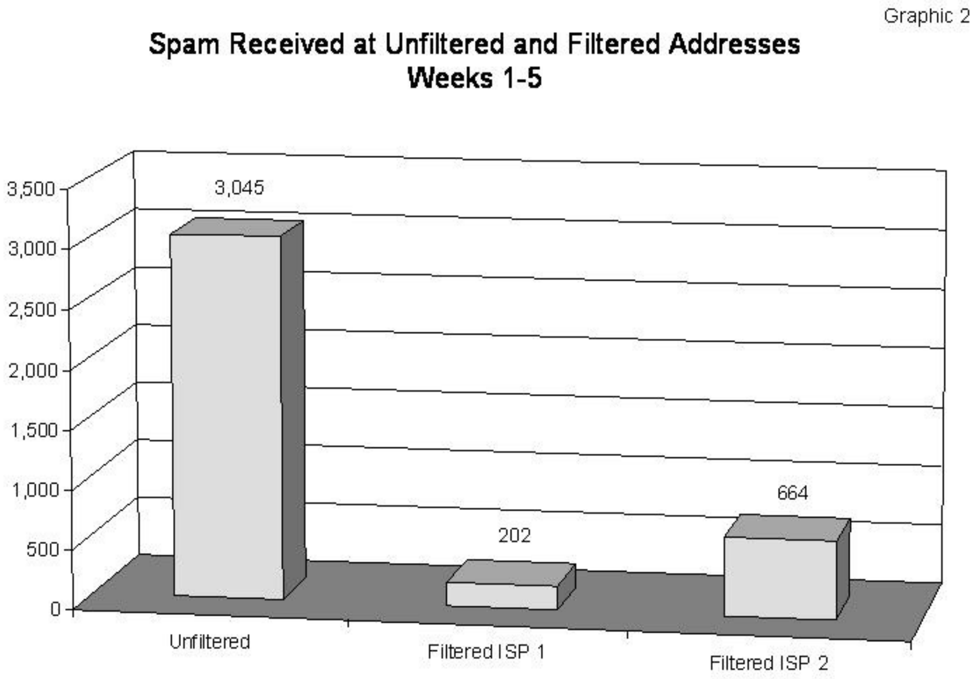
## III. Key Findings

### *Harvesting Continues to Occur, but ISPs' Spam-Filtering Technologies Continue to Play a Significant Role in Reducing the Amount of Spam Reaching Consumers' Inboxes*

Spammers continue to harvest email addresses. At the conclusion of the two week study period, the 50 Unfiltered Addresses had received a total of 718 pieces of spam. At the conclusion of the five week study period, these same addresses had received 3,045 pieces of spam. The total weekly amount of spam sent to the Unfiltered Addresses more than doubled from weeks one and two to weeks three through five.

Although FTC staff posted the 50 Unfiltered Addresses, the 50 addresses at Filtered ISP 1, and the 50 addresses at Filtered ISP 2 on the same 50 locations on the Internet, the Unfiltered Addresses received dramatically more spam than the addresses located at the two Filtered ISPs. After the two week study period, the 50 Unfiltered Addresses received a total of 718 spam messages, while the 50 addresses established at Filtered ISP 1 received 55 messages, and the 50 addresses established at Filtered ISP 2 received 231 messages. Thus, after two weeks, Filtered ISP 1 effectively prevented 92 percent of spam emails from entering its users' inboxes, and Filtered ISP 2 blocked 68 percent of spam messages.

After five weeks, the results were similar. While the 50 Unfiltered Addresses had received a total of 3,045 spam messages, the 50 addresses at Filtered ISP 1 had received a total of 202 messages, and the 50 addresses at Filtered ISP 2 had received 664 messages.



Thus, at the conclusion of the five week study period, Filtered ISP 1 effectively prevented 93 percent of spam messages from entering its users' inboxes, and Filtered ISP 2 blocked 78 percent of spam messages.

At the conclusion of both the two week and five week study periods, email addresses posted on particular types of Internet locations – such as websites - were far more likely to be harvested than email addresses posted on other types of Internet locations – such as message boards, chat rooms, blogs (and sites requesting comments or input from users) or social-networking websites. Indeed, the vast majority of the spam received was received by the

Unfiltered Addresses posted on website pages. At the conclusion of the two week study period, 86% percent of the total amount of spam messages received at Unfiltered Addresses were from addresses that had been posted on the FTC's website pages, and only 14% percent of the spam messages had been received from addresses posted elsewhere.

## IV. Conclusion

This study indicates that spammers continue to harvest email addresses posted on websites and, to a much lesser extent, those posted on other website locations such as chatrooms, message boards, social network sites, and video posting sites.

The fact that the vast majority of spam sent to harvested addresses in this study was never delivered to consumers' inboxes demonstrates the relative effectiveness of the two ISPs' spam filters. This result suggests that anti-spam technologies continue to have a significant impact on reducing the volume of spam delivered to consumers' inboxes.

# Appendix B

## Agenda

FEDERAL TRADE COMMISSION
601 NEW JERSEY AVE, NW
WASHINGTON, DC

Federal Trade Commission
July 11-12, 2007
Spam Summit
The Next Generation of Threats and Solutions

# AGENDA

## DAY 1-Wednesday, July 11, 2007

### 8:00 AM

Registration

### 9:00 AM

Introduction
Opening Remarks — Chairman Deborah Platt Majoras

### 9:15 AM

**Defining the Problem:** Earlier findings indicated that most spam was fraudulent, deceptive, and offensive. How has the nature of spam shifted? Is spam now being used for malicious and criminal purposes? Is this spam reaching consumers' inboxes or being filtered by Internet service providers' filtering software?

**Moderator:** Brian Huseman, Chief of Staff, Federal Trade Commission (FTC)

**Panelists:** Susannah Fox, Associate Director, Pew Internet & American Life Project
Thomas X. Grasso, Jr., Supervisory Special Agent, Federal Bureau of Investigation (FBI)
J. Trevor Hughes, Executive Director, Email Sender & Provider Coalition (ESPC)
Scott Richter, Chief Executive Officer, Media Breakaway, LLC
Charles E. Stiles, Chairman, Messaging Anti-Abuse Working Group (MAAWG)

### 10:45 AM

Break

### 11:00 AM

**Evolving Methods for Sending Spam and Malware:** To what extent, if any, have email address harvesting, dictionary attacks, and open proxies been replaced by botnets, zombies, and spam that uses images instead of text as the primary methods of spam distribution?

**Moderator:** Lawrence Hodapp, Attorney, Division of Marketing Practices, FTC

**Panelists:** Ben Butler, Director of Network Abuse, GoDaddy.com, Inc.
Patrick Peterson, Vice President, Technology, IronPort Systems
Jon L. Praed, Esq., Partner, Internet Law Group
Suresh Ramasubramanian, Manager, Antispam Operations, Outblaze Limited
Joe St Sauver, Ph.D., Manager, Internet2 Security Programs, Internet2 and the University of Oregon

12:30 PM

LUNCH (ON YOUR OWN)

1:45 PM

**UNCOVERING THE MALWARE ECONOMY:** What are the financial incentives for malicious spammers? What is the cost along the email chain to consumers, businesses, internet service providers, and networks?

**Moderator:** Sheryl L. Drexler, Investigator, Division of Marketing Practices, FTC

**Panelists:** Gregory Crabb, United States Postal Inspector, United States Postal Inspection Service
Jens W.L. Hinrichsen, Product Marketing Manager, Consumer Solutions, RSA, The Security Division of EMC
Andrew J. Klein, Senior Product Marketing Manager, SonicWALL, Inc.
Heinan Landa, President and Founder, Optimal Networks, Inc.

3:15 PM

BREAK

3:30 PM

EMERGING THREATS

**Moderator:** Sana Coleman Chriss, Attorney and Spam Coordinator, Division of Marketing Practices, FTC

**Panelists:** Michael Altschul, Senior Vice President and General Counsel, CTIA-The Wireless Association
Dave Champine, Senior Director, Product Marketing, Cloudmark, Inc.
Scott Chasin, Chief Technology Officer, MX Logic
Rick Lane, Vice President Government Affairs, News Corporation
Christopher J. Rouland, Chief Technology Officer, IBM Distinguished Engineer, IBM Internet Security Systems

## DAY 2-Thursday, July 12, 2007

8:00 AM

REGISTRATION

9:00 AM

ANNOUNCEMENTS

9:15 AM

**Deterring Malicious Spammers and Cybercriminals:** What are the investigatory challenges faced by law enforcement as spammers mask their identities and use obfuscatory techniques? What are effective countermeasures?

**Moderator:** Lois C. Greisman, Associate Director, Division of Marketing Practices, FTC

**Panelists:** Gene Fishel, Assistant Attorney General and Chief, Computer Crimes Section, Office of the Attorney General of Virginia
Aaron Kornblum, Senior Attorney, Microsoft Corporation
J. Keith Mularski, Special Agent, Federal Bureau of Investigation (FBI)
Robert Shaw, Head, ICT Applications and Cybersecurity Division, International Telecommunication Union (ITU)
Mona Sedky Spivack, Trial Attorney, U.S. Department of Justice - Criminal Division, Computer Crime and Intellectual Property Section (CCIPS)
Hugh Stevenson, Deputy Director, Office of International Affairs, FTC

10:45 AM

**Break**

11:00 AM

**Keeping it Out of the Inbox:** During the FTC's 2004 Email Authentication Summit, co-hosted with the Department of Commerce's National Institute of Standards and Technology, the FTC initiated efforts to spur the development and wide-scale adoption of domain level email authentication. Where does the implementation of email authentication stand? What are other key spam-reducing tools?

**Moderator:** Sana Coleman Chriss, Attorney and Spam Coordinator, Division of Marketing Practices, FTC

**Panelists:** Des Cahill, Chief Executive Officer, Habeas, Inc.
Jim Fenton, Distinguished Engineer, Cisco
Richard L. Gingras, Chairman, CEO and CoFounder, Goodmail Systems
Martha K. Landesberg, Director of Policy and Counsel, TRUSTe
Margot Koschier Romary, Senior Manager, Anti-Spam Operations, AOL
Craig Spiezle, Director, Online Safety Strategies and Technologies, Microsoft Corporation

12:30 PM

**Lunch** (on your own)

## 1:30 PM

**Putting Consumers Back in Control:** How can we empower consumers and businesses in the fight against spam and malware?

**Moderator:** Ruth Yodaiken, Attorney, Division of Marketing Practices, FTC

**Panelists:** Jeffrey Fox, Technology Editor, Consumer Reports
Dave Lewis, Vice President, Market and Product Strategy, StrongMail Systems, Inc.
Miles Libbey, Senior Product Manager, Yahoo! Mail, Yahoo!, Inc.
Linda Sherry, Director, National Priorities, Consumer Action

## 2:30 PM

**Break**

## 2:45 PM

**Identifying Best Practices for Businesses:** What can businesses do to distinguish themselves from malicious spammers?

**Moderator:** Phillip Tumminio, Attorney, Division of Marketing Practices, FTC

**Panelists:** Matt Blumberg, Founder and CEO, Return Path
Jerry Cerasale, Senior Vice President, Government Affairs, Direct Marketing Association, Inc.
John Ingold, Director, Security and Risk Assessment, BITS
John Mathew, Vice President, Operations, Epsilon
Alastair Tempest, Director General, Federation of European Direct and Interactive Marketing (FEDMA)
Mike Zaneis, Vice President, Public Policy, Interactive Advertising Bureau (IAB)

## 4:00 PM

**Developing a Plan for Action**

**Moderator:** Dan Salsburg, Assistant Director, Division of Marketing Practices, FTC

**Panelists:** Thomas X. Grasso, Jr., Supervisory Special Agent, Federal Bureau of Investigation (FBI)
Miles Libbey, Senior Product Manager, Yahoo! Mail, Yahoo!, Inc.
Brendon Lynch, Director of Privacy Strategy, Trustworthy Computing Group, Microsoft Corporation
Michael O'Reirdan, Distinguished Engineer in National Engineering and Technical Operations, Comcast Corporation
Phyllis A. Schneck, Ph.D., Chairman, Board of Directors, InfraGard National Members Alliance and Vice President, Research Integration, Secure Computing Corp.
Charles E. Stiles, Chairman, Messaging Anti-Abuse Working Group (MAAWG)